IN THE DRAWINGS

The attached sheets of drawings include changes to Figs. 2, 12-14, 16 and 21A. These sheets, which include Figs. 2, 12-14, 16 and 21A, replace the original sheet including Figs. 2, 12-14, 16 and 21A.

Attachment: Replacement Sheets

REMARKS/ARGUMENTS

Favorable consideration of this application, as presently amended, is respectfully requested.

Claims 1-10, 12, 14, 15 and 17-25 are pending in the present application. Claims 1-3, 5-10, 12, 15 and 17-23 are amended, Claims 11, 13 and 16 are cancelled and Claims 24-25 are added. Support for additions and amendments to the claims is found in the disclosure as originally filed, at least in Figure 11A. Thus, no new matter is added.

In the outstanding Action, the title was objected to as including informalities; Claims 21-23 were rejected under 35 U.S.C. §101, as directed to non-statutory subject matter; Claims 1, 5-10 and 12-23 were rejected under 35 U.S.C. §103(a) as unpatentable over Newcombe (U.S. Pat. Pub. No. 2003/0172269) in view of Arnold et al. (WO 03/055170, herein "Arnold"); and Claims 2-4 and 11 were rejected under 35 U.S.C. §103(a) as unpatentable over Newcombe and Arnold in view of Medvinsky et al. (U.S. Pat. Pub. No. 2003/0063750, herein "Medvinsky").

With respect to the objection to the title, the title has been amended to overcome the objection. Accordingly, Applicants respectfully request that the objection to the title be withdrawn.

With regard to the rejection of Claims 21-23 under 35 U.S.C. §101 as directed to non-statutory subject matter, Claims 21-23 have been amended to overcome the rejection. Specifically, these claims have each been amended to recite a computer readable storage medium claim. Accordingly, Applicants respectfully request that the rejection of Claims 21-23 under 35 U.S.C. §101 as directed to non-statutory subject matter be withdrawn.

Addressing now the rejection of Claims 1, 5-10 and 12-23 under 35 U.S.C. §103(a) as unpatentable over Newcombe and Arnold, Applicants respectfully traverse this rejection.

Claim 1 recites,

In an authentication system in which an authentication server which authenticates a user, a user terminal which transmits a user authentication information, and an application server which provides a service to the user through the user terminal are connected together to enable a communication therebetween through a network; an address based authentication system in which

the authentication server comprises

authentication means for authenticating a user based on the user authentication information transmitted as an authentication request from the user terminal;

an address allocating means for allocating an address to the user terminal for a successful authentication of the user;

authentication information generating means for generating information for authentication from information including the allocated address;

a ticket issuing means for issuing a ticket containing the allocated address allocated by the address allocating means and the information for authentication;

and a ticket transmitting means for transmitting the ticket issued by the ticket issuing means to the user terminal;

the user terminal comprises

a user authentication information transmitting means for transmitting [[a]] user authentication information to the authentication server for purpose of an authentication request;

a ticket reception means for receiving the ticket containing the allocated address transmitted from the authentication server;

means for setting up the allocated address contained in the ticket as a source address for a packet which is to be transmitted from the user terminal;

means for transmitting a packet including the ticket to the application server for establishing a session;

and a service request means for transmitting a packet requesting a service to the application server through the session;

and the application server comprises

a ticket memory means for storing the ticket transmitted from the user terminal;

ticket verifying means for verifying the presence or absence of any forgery in the information for authentication in the ticket transmitted from the user terminal and storing the ticket in the ticket memory means in the absence of a forgery;

an address comparison means for determining whether or not the allocated address contained in the ticket which is stored in the ticket memory means coincides with the source address of the service request packet which is transmitted from the user terminal through the session;

and a service providing means for transmitting to the user terminal packets which provides a service to the user when

> a coincidence between the addresses is determined by the address comparison means.

Newcombe describes an application authentication system (AAS) that authenticates a client in response to the client's request, and sends a content ticket containing local and remote IP addresses to the client. Further, in the system of Newcombe, the client sends the content ticket to a content server as a content request. In response, the content server checks if the IP address in the received content ticket matches the source address of the received packet which contains the content ticket. If they match, the content server transmits the content to the client. That is, if both addresses match each other, it is decided that the content ticket is authentic and the content is sent to the client's IP address without checking the authenticity of the IP address. In other words the authenticity of the IP address is not checked in terms of whether or not the address is allocated by an organization such as an ISP through a correct procedure which includes authentication of a user.

However, Newcombe does not describe or suggest an authentication server including authentication information generating means for generating information for authentication from information including the allocated address and a ticket issuing means for issuing a ticket containing the allocated address allocated by the address allocating means and the information for authentication, as is recited in Claim 1.

In other words, Newcombe discloses the issuance of a ticket containing an IP address, but does not disclose allocation of an address to ***the authenticated user*** by the authentication server. In addition, Newcombe does not describe or suggest including in the ticket an address which is guaranteed to be an authentic address allocated to the authenticated user. In contrast, in Newcombe, the address is included in a ticket regardless of the authenticity of the address. Furthermore, Newcombe does not teach anything about ticket memory means provided in the application server.

Therefore, the system of Newcombe cannot check the authenticity of an address in the header of each subsequent packet. This is the case, at least, because Newcombe does not have any intention of checking address consistency for those packets subsequent to the packet containing a ticket and, therefore, there is provided no means for storing the ticket containing the allocated address.

Thus, Applicants respectfully submit that Claim 1 patentably distinguishes over Newcombe. Nevertheless, Applicants respectfully submit that the outstanding Action cites Arnold as curing the deficiencies of Newcombe with regard to the claimed invention.

Arnold describes a system that includes a server which authenticates a user and allocates the user an IP address. Further, in Arnold a session is established between the server and a user computer. In addition, the server always monitors the user's access to the network through the session so that authentication can be achieved between the user and a service provider through the session.[1]

However, Arnold does not describe or suggest an authentication server including authentication information generating means for generating information for authentication from information including the allocated address and a ticket issuing means for issuing a ticket containing the allocated address allocated by the address allocating means and the information for authentication, as is recited in Claim 1.

In other words, Arnold does not produce a ticket containing an IP address, and the way of guaranteeing the validity of an IP address differs from the claimed invention.

Moreover, Applicants note that a combination of Newcombe and Arnold would not operate as is suggested by the outstanding Action (i.e. to guarantee authentication). Specifically, in Newcombe, it is a precondition that an IP address be determined prior to communication. This is apparent from the fact that the well-known authentication system

[1] See page 4, second and third paragraphs of Arnold.

(i.e. Kerberos) which is referred to in Newcombe, and is similar to Newcombe, has been designed under such a precondition. Therefore, if Newcombe and Arnold were to be combined (taking into account their preconditions) the system would operate as follows.

First, a user would be authenticated and an IP address would be allocated to the user terminal as taught in Arnold. Then, the user terminal would present the allocated address to AAS, which in turn would send a ticket containing the IP address to the terminal as taught in Newcombe.

However, in this combination it would not be possible to guarantee, for the application server, the validity of IP address contained in the ticket. That is the case, because the user authentication, IP address allocation and issuance of a ticket assuring the validity of the ticket (address contained in a ticket in such a form as to guarantee that the address is a valid one allocated to the authenticated user) are not implemented collectively based on user authentication and therefore no guarantee of authenticity of the address and assurance of a packet from an authenticated user can be attained.

Moreover, Newcombe's purpose is to ascertain consistency of address as is the case in any Kerberos system. However, even if the IP address were used consistently in the protocol, it would not be possible to ascertain whether the address has been allocated justly to the user terminal based on authentication. Therefore, it is not possible to conduct safe authentication based on such an IP address. For example, an arbitrary node (i.e. such as a deceptive access point) on a path between an authenticated user terminal and a server would be able to impersonate the user terminal using the IP address of the user terminal.

Thus, Newcombe does not provide the advantageous features of the claimed invention.

Similarly, Arnold does not cure the deficiencies of Newcombe at least because Arnold adopts a different technique from the claimed invention. For instance, the system of Arnold

has no need for the issuance of tickets. Moreover, the system of Arnold requires significant load on the authentication server.

Moreover, in Newcombe, the application server does not have a ticket memory means. That is, for the packet containing a ticket, it is possible to check the consistency of address; however, for those subsequent packets, it is not. This is understandable considering that in Newcombe an IP address is contained in a ticket and authenticity of the ticket is validated by checking address consistency. Once the ticket is found authentic, there is no need to keep the ticket. As a result, Newcombe does not require a ticket memory means.

On the other hand, in the claimed invention, a ticket is sent to an application server to ensure the authenticity of the IP address for each sequence of a packet transmitted from a user terminal to the application server in the same session. That is, not only the packet containing a ticket but also the subsequent packets must be authenticated. Therefore, it is necessary to provide a ticket memory means.

Accordingly, Applicants respectfully submit that Claim 1 patentably distinguishes over Newcombe and Arnold considered individually or in combination.

With regard to Claim 7, Applicants respectfully submit that Claim 7 also patentably distinguishes over Newcombe and Arnold.

Specifically, the outstanding Action acknowledges on page 10 that the address allocating means recited in Claim 7 is not disclosed in Newcombe. Nevertheless, the outstanding Action asserts that this feature is described on page 5, lines 25-29 of Arnold, Applicants respectfully traverse this assertion. Specifically, Applicants note that Arnold does not use tickets and therefore does not teach anything about containing an allocated address in a ticket.

Moreover, Claim 7 has been amended by the present response to incorporate therein the features of Claims 8 and 11. With regard to these features (particularly the features

previously recited in Claim 11), Newcombe discloses in paragraph [0072] that a content ticket may include a session key. A session key which is shared by a client and a server is usually supplied from the server to the client. However, in the invention recited in Claim 7, information relating to a user terminal's public key is contained in the ticket. It is this information that is supplied from the user terminal. The outstanding Action acknowledges on page 22 that Newcombe and Arnold do not describe or suggest this feature. Nevertheless, the outstanding Action asserts that Medvinsky teaches the feature of "key information relating to a public key of the user terminal is contained in the authentication request," recited in amended Claim 7. However, Applicants respectfully traverse this assertion and submit that Medvinsky merely describes in paragraph [0023] that the ticket granting ticket TGT is authenticated by a public key previously registered with the provisioning ticket. This description does not correspond to the claimed feature recited in amended Claim 7.

In addition, as is noted above, the features of Claim 8 are incorporated into Claim 7. With regard to these features, Newcombe discloses in paragraph [0065] that the TGS (ticket granting server) in the application authentication system (AAS) generates a signature on the client readable portion of a content ticket using the authentication server's private key. However, Applicants note that the technology of generating a signature using a private key (the signature can be verified using a public key corresponding to the private key) is different from the technology of generating information for authentication using a shared secret key (information for authentication can be verified only by the shared key). Moreover, it should be noted that the client readable portion of the content ticket in Newcombe is directed to a client, while in amended Claim 7, the information for authentication is directed to the application server.

Further, regarding the feature of "the ticket issuing means being means for issuing the ticket inclusive of the authentication information," the ticket according to Newcombe does

not contain anything equivalent to the information for authentication generated by processing information including the allocated address and key information using the shared secret key which is shared between the authentication server and the application server.

Accordingly, Applicants respectfully submit that amended Claim 7 patentably distinguishes over Newcombe, Arnold and Medvinsky.

With regard to Claim 12, Applicants respectfully submit that Claim 12 also patentably distinguishes over Newcombe and Arnold.

Applicants note that Newcombe does not describe or suggest the source address set-up means recited in Claim 12 in addition to the above noted arguments which relate to the features of the ticket reception means. Moreover, Applicants note that the features of Claim 13 have been incorporated into Claim 12 and thus Applicants respectfully submit that this claim patentably distinguishes over Newcombe and Arnold on this basis as well.

Specifically, Newcombe discusses in paragraph [0029] about various types of encryption keys, but does not describe the key information generating means for generating a key information from the user terminal's public key, and the user authentication transmitting means for transmitting the key information together with the user authentication information. Moreover, Arnold does not cure this deficiency of Newcombe.

Thus, Applicants respectfully submit that amended Claim 12 patentably distinguishes over Newcombe and Arnold.

With regard to Claim 15, Applicants respectfully submit that Claim 15 also patentably distinguishes over Newcombe and Arnold.

Applicants note that Newcombe does not disclose or suggest either ticket memory means for storing the ticket when the ticket is verified authentic or address comparison means which compares the source address of a service request packet with the allocated address in the ticket stored in the ticket memory means. Moreover, amended Claim 15, recites that

authenticity of the received ticket is checked and, if satisfied, the ticket is stored in the ticket memory means and, thereafter, in response to a service request packet from the user terminal, the source address of the service request packet is compared to the address in the ticket stored in the ticket memory means. Whereby it is possible for the application server to identify the service-requesting user based on the addresses and authentication of the destination address to which the service should be forwarded can be assured. Moreover, Arnold does not cure this deficiency of Newcombe.

In addition, Applicants note that the features of Claims 16 and 17 have been incorporated into Claim 15. With regard to these features, Newcombe does not teach anything about preventing the ticket from being stored in the ticket memory means when the ticket is found to be not authentic. Moreover, Arnold does not cure this deficiency of Newcombe.

Thus, Applicants respectfully submit that amended Claim 15 patentably distinguishes over Newcombe and Arnold.

Moreover, with regard to dependent Claim 2 Applicants respectfully submit that this claim also patently distinguishes over Newcombe, Arnold and Medvensky irrespective of this claims dependence from Claim 1.

Specifically, regarding the ticket issuing means, Newcombe's paragraph [0068] describes the TGT and does not teach anything about a content ticket containing key information which is related to a public key and received from a client. Further with regard to the user authentication information transmitting means, Newcombe's paragraph [0052] describes that a client provides an AAS (application authentication system) with the information relating to local and remote IP addresses as a request for a content ticket, but does not disclose sending the key information together with the user authentication information. With regard to the session key generating means, Newcombe's paragraph [0029]

discusses various types of encryption keys, but does not describe calculating a session secret key from a user terminal's private key and an application server's public key. With regard to the packet cryptographic processing means, Newcombe's paragraph [0065] describes extracting a session key from the client readable portion of the TGT and encrypting the subsequent authenticators with the session key, but does not describe processing a packet with the session key and verifying the packet. With regard to the packet verifying means, Newcombe's paragraph [0065] describes a server which extracts a session key from a server readable portion and decrypts the authenticator; however, there is no description of a packet verifying means for confirming, using the session secret key, whether or not the packet received from the user terminal is forged or a ticket verifying means for verifying whether or not the key information contained in the ticket of the packet, which has been verified as not being forged, is information relating to the public key of the user terminal, and if not, preventing the ticket from being stored in the ticket memory means. With regard to the ticket verifying means, Newcombe's paragraph [0086] describes that "if the client is unsuccessful, the processing ends", however there is no description of preventing the ticket from being stored in the ticket memory means.

With regard to the feature that the user terminal has a key information relating to a public key of the user terminal, Applicants note that this feature also is not disclosed by the cited references.

Specifically, the cited Medvinsky reference relates to a method for securely sending a client's public key to a key distribution center (KDC, acting as authentication server), wherein KDC generates a provisioning key related to client's ID and provides the key to a provisioning server, which in turn generates a configuration parameter for initialization of the client so as to contain the provisioning key and provides the parameter to the client, which in turn generates key pair according to the parameter and sends the public key to KDC, which in

turn authenticates the public key with the provisioning key, whereby it is assured that the public key is certainly not forged.

Further, in Medvensky, transmission of a public key to KDC is secured using the provisioning key. In contrast, in Claim 2, key information related to a public key is transmitted along with information for authentication from a user terminal to an authentication server and if authentication is successful, the authentication server issues a ticket containing key information to the authenticated user.

According to Medvinsky, the public key transmitted by the client may be sent correctly to the server, but since there is no authentication of the user for the transmission, there is no assured relation between the user and the public key. In Medvensky, the provisioning key sent from a server to a client can authenticate a message but cannot authenticate the user.

In Claim 2, a user is authenticated by the authentication server using the user's key, and key information is contained in the ticket issued to the authenticated user. Therefore, the correspondence between the authenticated user and the public key of the user's terminal is assured by the ticket.

Furthermore, there is a difference in how the public key is used in Medvensky. For example, in Medvensky the public key is used between a user terminal and an authentication server for authentication of a message transmitted from the user terminal to the authentication server. Thus, the public key will never be included in a ticket for distribution.

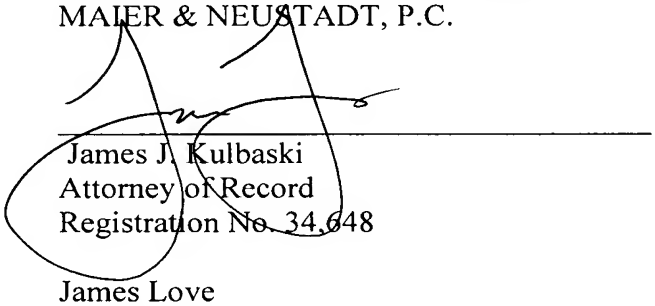
In contrast, in Claim 2, the public key is included in a ticket by the authentication server and the ticket is sent to the user terminal, and the public key is used between the user terminal and the ***application server***.

Accordingly, Applicants respectfully submit that amended Claim 2 patentably distinguishes over Newcombe, Arnold and Medvinsky.

Consequently, in view of the present amendment, no further issues are believed to be outstanding in the present application, and the present application is believed to be in condition for formal Allowance. A Notice of Allowance for the claims is earnestly solicited.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



James J. Kulbaski
Attorney of Record
Registration No. 34,648

James Love
Registration No. 58,421

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

I:\ATTY\JL\271813US\271813US_AMR.DOC